Security Architecture Work Group
Of the
Nebraska Information Technology Commission
Tuesday October 31, 2000
1:30 p.m. to 4:30 p.m.
Nebraska State Office Building,
Lower Level, Conference Room C
301 Centennial Mall South
Lincoln, Nebraska

Minutes

A. Participants

Rod	Armstrong	Nebraska Online
Mahendra	Bansal	Natural Resources
Steve	Cherep	HHSS/IS&T
Margo	Gamet	HHSS/IS&T
Jerry	Hielen	IMServices
Scott	McFall	State Patrol
George	McMullin	Corpnet Security/Nebraska Cert
Michael	Overton	Crime Commission
Leona	Roach	University of Nebraska Computing Services Network
Steve	Schafer	Nebraska CIO
Marlea	Thompson	Labor
Mark	Urbach	Education
Walter	Weir	University of Nebraska CIO

B. Review Proposed Timeline and Process

Steve Schafer outlined the process envisioned in the Statewide Technology Plan. Since the last meeting of the Security Architecture work group, the Technical Panel accepted the draft policies for consideration. This triggered a 30-day review and comment period, which expired October 20. Several people sent suggestions, which were distributed with the notice of today's meeting. After the work group finishes the draft policies, the Technical Panel will decide whether to recommend them to the NITC. The Technical Panel would act on the draft policies at its December meeting. Assuming that happens, the NITC may consider the policies at their January meeting.

C. Discussion and Recommendations on the Draft Security Policies

The work group participants discussed each of the comments submitted during the review and comment period. The work group accepted many of the comments, which will be reflected in the final draft of the security policies. Some of the changes included the following:

1. Security Management Policy
   - Be consistent with other policies and refer only to section 86-1506(6) under the Authority section. The other references will be added to section G, "Related Polices, Standards, and Guidelines."
   - Under standards, clarify that "compliance" will refer to consequences of violations.

- Under standards, add a requirement for data classification to determine the appropriate level of security.

2. Access Control Policy
   - Revise the standard for passwords to require "at least 5 alphanumeric characters…" with no upper limit. Recommend renewing passwords "at least every six months."
   - Under standard number 14, workstation security, delete the second, redundant recommendation that sensitive or critical information should not be stored on workstations.
3. Disaster Recovery Policy
   - Emphasize that disaster recovery includes business resumption, not just data backups. Also emphasize the importance of testing and improvement of the disaster recovery plan.
4. Education, Training, and Awareness Policy
   - Include the need to provide training on the potential consequences of security violations.
5. Individual Use Policy
   - Under standards, include a requirement that "agencies should develop policies regarding monitoring e-mail, Internet use, and other computer resources. The policies should identify the circumstances under which monitoring will occur and who may authorize such monitoring."
   - Modify item (h), under Acceptable Use, to prohibit "Unsolicited advertising, unless authorized by the governing body of the organization."
6. Network Security Policy
   - Delete item (k), under General Network Controls, because it repeats item (d).
   - Add a requirement to manage security according to "the security needs of other agencies or institution connected to the network."
7. Security Breaches and Incident Reporting Policy
   - Add a section that acknowledges that not all agencies have the resources to conduct their own intrusion detection and analysis. In these situations, it may be necessary to identify other sources for assistance in tracking and responding to incidents. It is important to have a clear understanding of when to escalate an issue.
   - Delete the word "secondary" wherever it appears in the section on standards, because it give s misleading impression on the importance of other goals.

Several comments dealt with the need for templates and other assistance to agencies as they try to implement broad security policies. This is particularly true of small agencies. The work group agreed to address this issue as part of a later effort to prepare a security implementation plan.

One reviewer emphasized the need for a common data classification system. After much discussion, with viewpoints on both sides of the issue, the work group decided to include a clear directive regarding the need for data classification, but not adopt a single classification system that would apply to all. The argument against a single data classification system centered on the need to involve the business perspective of agency management in developing the data classification system. It will be hard enough for some agencies to develop a data classification system. Involving all agencies in a joint effort would make the task even harder and would take considerable time. The work group decided to address this issue in greater detail in an implementation plan / best practices.

Another set of comments suggested an entirely different approach to security policies. The reviewer recommended that "a statewide security policy should provide a charter for implementing security, and be fairly short, approximately three to five pages." The comments provided an outline for the content and organization of security policies, risk management, compliance, management, and other issues. The work group decided not to rewrite the current security policies, but recommended that we incorporate the suggestion for a more compact document by developing an electronic version of the

security policies, which presents the boiler plate sections (sections D, E, F, and G) as a single set of links. The outline for content and organization of security issues will be considered when developing an implementation plan / best practices document.

The work group decided to address several other suggestions in an implementation plan / best practices document. These include:

- Sample documents for agencies to use
- More detailed procedures that agencies can adopt and modify
- Guidelines and best practices for intrusion detection, reporting and investigations
- Guidelines and best practices for monitoring individual activity, such as e-mail and Internet
- Guidelines and best practices for managing passwords or other access at different levels (application level, hardware, login, network, etc.)

D. Implementation Issues

The work group discussed how to implement these security policies. Discussion included the need for executive sponsorship, such as involving the Governor and briefing the Legislature. Participants mentioned the need for training and disseminating best practices. The work group agreed on the idea of sponsoring a security workshop next spring. The workshop would provide training on the major topics of security. The organization of the workshop could mirror the table of contents of a security manual / best practices document. One possible outcome would be to use the workshop to prepare such a document.

The next meeting of the workgroup will focus on implementation issues. No meeting date was set.